What is claimed is:

1. (Previously Presented) A cryptographic feature enablement system comprising:

a CPU;

a bus operably and directly connected to said CPU;

at least one non-volatile read/write memory operably connected to said bus and accessible by said CPU;

a cryptographic chip having disposed therein at least one cryptographic system and algorithm, and further operably connected to said bus and accessible by said CPU;

an encrypted token operably disposed within said at least one non-volatile read/write memory and further configured to contain encrypted initialization data for enabling a desired set of cryptographic capabilities corresponding to said cryptographic chip;

system-specific information assigned to an individual system and readable by said CPU; and,

a token decryption system operably disposed within said at least one non-volatile read/write memory configured to enable and use said cryptographic chip and said system-specific information to decrypt said encrypted initialization data in said encrypted token, and further configured to reconfigure said cryptographic chip in accordance with said initialization data in said token and in accordance with said system-specific information responsive to said encrypted initialization data being decrypted.

2. (Original) The cryptographic feature enablement system of claim 1 where said at least one non-volatile read/write memory comprises FLASH memory.

3. (Original) The cryptographic feature enablement system of claim 1 where said system-specific information is the system's MAC address.

4. (Original) The cryptographic feature enablement system of claim 3 where said MAC address is used to generate a private key.

5. (Previously Presented) A method for initializing cryptographic functionality in a system, the method comprising:

starting the boot process in a system;

using said system's system-specific information to generate a key;

decrypting an encrypted token using said key wherein said encrypted token includes encrypted encryption initialization data;

establishing if said decrypted encryption initialization data from said encrypted token is useable for a cryptographic chip in said system;

initializing said cryptographic using said decrypted encryption initialization data responsive to a determination that said encryption initialization data is usable; and,

initializing said cryptographic chip in accordance with a default if said decrypted token is not usable.

6. (Original) The method of claim 5 where said default initialization is to immediately bring the system back down.

7. (Original) The method of claim 5 where said default initialization is to bring the system up with no cryptographic capabilities enabled.

8. (Original) The method of claim 5 where said system-specific information is said system's MAC address.

9. (Previously Presented) A program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine for initializing cryptographic functionality in a system, the method comprising:

starting the boot process in a system;

using said system's system-specific information to generate a key;

decrypting an encrypted token using said key wherein said encrypted token includes encrypted encryption initialization data;

establishing if said decrypted encryption initialization data from said encrypted token is useable for a cryptographic chip in said system;

initializing said cryptographic chip using said decrypted encryption initialization data responsive to a determination that said encryption initialization data is usable; and,

initializing said cryptographic chip in accordance with a default if said decrypted token is not usable.

10. (Original) The method of claim 9 where said default initialization is to immediately bring the system back down.

11. (Original) The method of claim 9 where said default initialization is to bring the system up with no cryptographic capabilities enabled.

12. (Original) The method of claim 9 where said system-specific information is said system's MAC address.

13. (Previously Presented) A system for initializing cryptographic functionality in a system, the system comprising:

means for starting the boot process in a system;

means for using said system's system-specific information to generate a key;

means for decrypting an encrypted token using said key;

means for decrypting an encrypted token using said key wherein said encrypted token includes encrypted encryption initialization data;

means for establishing if said decrypted encryption initialization data from said encrypted token is useable for a cryptographic chip in said system;

means for initializing said cryptographic using said decrypted encryption initialization data responsive to a determination that said encryption initialization data is usable; and,

means for initializing said cryptographic chip in accordance with a default if said decrypted token is not usable.

14. (Original) The system of claim 13 where said default initialization is to immediately bring the system back down.

15. (Original) The system of claim 13 where said default initialization is to bring the system up with no cryptographic capabilities enabled.

16. (Original) The system of claim 13 where said system-specific information is said system's MAC address.

17. (Original) A method for installing cryptographic initialization data in a system for use during system booting, the method comprising:

identifying the system-specific information of said system;

generating at least one key using said system-specific information;

using one key of said at least one keys to encrypt a token, where said token comprises cryptographic initialization data applicable to said system; and,

writing said encrypted token in non-volatile memory in said system, where said non-volatile memory is configured to be accessible by a CPU in said system during system initialization.

18. (Original) The method of claim 17 where said non-volatile memory is FLASH memory.

19. (Original) The method of claim 17 where said generation of at least one key further comprises generating a public key and a private key, and choosing said public key to encrypt said token and choosing said private key to use for decrypting said token.

20. (Original) The method of claim 17 where said system-specific information is said system's MAC address.

21. (Original) A program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine for installing cryptographic initialization data in a system for use during system booting, the method comprising:

identifying the system-specific information of said system;

generating at least one key using said system-specific information;

using one key of said at least one keys to encrypt a token, where said token comprises cryptographic initialization data applicable to said system; and,

writing said encrypted token in non-volatile memory in said system, where said non-volatile memory is configured to be accessible by a CPU in said system during system initialization.

22. (Original) The method of claim 21 where said non-volatile memory is FLASH memory.

23. (Original) The method of claim 21 where said generation of at least one key further comprises generating a public key and a private key, and choosing said public key to encrypt said token and choosing said private key to use for decrypting said token.

24. (Original) The method of claim 21 where said system-specific information is said system's MAC address.

25. (Original) A system for installing cryptographic initialization data in a system for use during system booting comprising:

means for identifying the system-specific information of said system;

means for generating at least one key using said system-specific information;

means for using one key of said at least one keys to encrypt a token, where said token comprises cryptographic initialization data applicable to said system; and,

means for writing said encrypted token in non-volatile memory in said system, where said non-volatile memory is configured to be accessible by a CPU in said system during system initialization.

26. (Original) The system of claim 25 where said non-volatile memory is FLASH memory.

27. (Original) The system of claim 25 where said means for generation of at least one key further comprises generating a public key and a private key, and choosing said public key to encrypt said token and choosing said private key to use for decrypting said token.

28. (Original) The system of claim 25 where said system-specific information is said system's MAC address.